

Michael Yuan, Second State: The Default Should be Zero Trust

• 5 minutes to read

[Original post from CyberNews](#)

Whether constructing a new cloud-native app or updating an existing one, developers should keep to an even set of principles.

The application optimization cycle becomes critical if keeping up with consumer expectations and agile business operations are desired to be achieved. Harnessing the full power of the cloud can not only reduce costs but also visibly improve the everyday user experience. Therefore, building native cloud applications should become a priority.

Today, our researchers contacted Michael Yuan, CEO of [Second State](#) – a company developing a lightweight, fast, and extensible code runtime for the edge and microservices– to find out the main challenges surrounding edge computing, whether [choosing a VPN](#) can help protect you on the cloud, and much more.

How did Second State originate? What has your journey been like?

Second State was created in 2019 to develop and commercialize a new open-source WebAssembly runtime (WasmEdge) specifically designed and optimized for cloud-native applications. We now have a thriving open source community (3000+ GitHub stars and over 100 code contributors), and many users/customers including several Fortune 500 companies.

WasmEdge is poised to become the next-gen lightweight application container to bring the cloud-native computing paradigm to a variety of applications from edge cloud, edge devices, and SaaS, to the blockchain.

Can you introduce us to what you do? What are the main issues you help solve?

WasmEdge is the WebAssembly runtime for cloud-native applications. It supports extensions, API, and features that are relevant to server-side applications, such as making [non-blocking network connections](#), accessing databases, using GPU to [execute AI models](#), running under [Kubernetes](#), and supporting JavaScript / Python apps.

Compare with traditional cloud-native containers, WasmEdge is much lighter, faster, safer, more portable, and can still be managed by the existing container and K8s toolchains, making it ideal for the resource-contained edge cloud or edge devices.

Here are some concrete examples of WasmEdge applications:

- Microservices and serverless functions in Kubernetes clusters
- Embedded functions in SaaS or cloud databases
- Application runtimes on mobile devices
- Smart contract runtimes on blockchains

It is evident that open source is an important part of Second State. Would you like to share more about your vision?

First, I firmly believe that all infrastructure software will be open source. Open source is the only way to get other developers in the community to try your software and collaborate on it.

We donated WasmEdge to the CNCF as a community project in 2021. Since then, our open source community has thrived and created many inbound business opportunities for Second State. Today, all Second State's customers and business development pipelines are from the WasmEdge open source community.

How did the recent global events affect your field of work? Have you noticed any new security issues arise as a result?

The pandemic delayed new software adoption. People tend to buy what they already know at a time of uncertainty. That has a negative impact on WasmEdge adoption. However, since late 2021, there has been an explosion of developer interest for server-side or cloud-native WebAssembly in the post-pandemic world. WasmEdge is on the leading edge of this wave.

In terms of security issues, we actually think WebAssembly is a great tool for making the software supply chain more secure. WebAssembly is secure by default with a capability-based security model and it has a very small attack surface. It requires apps to be built from its own toolchains providing opportunities to promote security best practices and supporting modern binary signing protocols. WebAssembly itself has diversified implementations.

What are the main challenges surrounding edge computing?

The challenges of edge computing are three folds. First, the edge environments are resource-constrained. Edge applications must be optimized for speed and resource consumption. That means standard VMs or containers must give way to lightweight or embedded runtimes.

Second, edge infrastructure often needs to support multi-tenancy. Security and resource isolation are critical for edge applications.

Third, edge servers and devices must support heterogeneous OSes and hardware. Cross-platform portability is important.

We believe WebAssembly runtimes, such as WasmEdge, are very well positioned to tackle those challenges.

What are the best practices companies should follow when developing, and, when launching applications?

I think the most important requirement for any product is the ability to address a market need. For example, the WasmEdge product enables developers to apply the cloud-native and serverless approach (ie containerization) to resource-constrained edge or SaaS applications.

What vulnerabilities do you find the most concerning at the moment?

The software industry is moving toward native clients (NaCl) written in modern languages like Go and Rust. The driver for this shift is the end of the Moore's Law era. However, the main challenge for native applications is that they cannot run securely in a multi-tenancy environment.

That's why we need a secure sandbox (i.e. WebAssembly) designed from the ground up to support compiled applications with a capability-based security model, support for modern software verification and signing tools, and a small attack service.

In this age of ever-evolving technology, what do you think are the key security measures everyone should implement on their devices?

I think we need to put all software components into secure sandboxes or containers. The default should be zero trust. When the application requires access to system resources outside of the sandbox, it needs to explicitly declare its requirements and then prove its identity through digital signatures. In order words, we should build the WebAssembly sandbox into every edge device and edge server.

Would you like to share what's next for Second State?

The Second State will develop, maintain, and promote the WasmEdge project. We will build on the WebAssembly standard, and continue to develop features and extensions needed by cloud-native application developers. We are also going to help users in our community deploy WasmEdge as a lightweight container for their own applications.

Second State will launch its own WasmEdge-powered cloud services for the community. A serverless function-as-a-service platform [Flows](#) for specialized use cases. Stay tuned!

The success of any open source project depends on its community. We would love to see more engagements and contributions from users and developers in our community. Please go to our [GitHub repo](#), star it, read the docs, check out open issues, join the discussion board, and become part of the WasmEdge community!

We look forward to seeing you there!

Join WasmEdge Discord Server to [learn more](#).

[Edge Computing](#) [edge cloud](#) [WasmEdge](#) [#Rust](#)



A high-performance, extensible, and hardware optimized WebAssembly Virtual Machine for automotive, cloud, AI, and blockchain applications

[second-state](#) [@secondstateinc](#)